SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

December 2022, Vol. 65 222302:1–222302:21
https://doi.org/10.1007/s11432-021-3410-2

Physical layer authentication in UAV-enabled relay networks based on manifold learning

Shida XIA[1], Xiaofeng TAO[1*], Na LI[1,2], Shiji WANG[1] & Jin XU[1]

[1]*National Engineering Lab for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing* 100876*, China;*
[2]*Beijing University of Posts and Telecommunications Research Institute, Shenzhen* 518000*, China*

Received 15 July 2021/Revised 22 October 2021/Accepted 13 January 2022/Published online 21 November 2022

Abstract An unmanned aerial vehicle (UAV) relay network is a promising solution in the next-generation wireless networks due to its high capacity and unlimited geography. However, because of the openness of wireless channels and UAV mobility, it is remarkably challenging to guarantee the secure access of UAV relay. In this paper, we investigate the physical layer authentication (PLA) to verify the identity of the UAV relay for preventing unauthorized access to users' information or network service. Unlike most existing PLA methods for UAV, the proposed PLA scheme fully considers the time-varying of physical layer attributes caused by UAV mobility, and transforms the authentication problem into recognizing nonlinearly separable physical layer data. Particularly, we propose a manifold learning-based PLA scheme that can authenticate the mobile UAV relay in real time by establishing the local correlation of physical layer attributes. The Markov chain of physical layer data in the time domain is established to evaluate UAV state transition probability through the proposed diffusion map algorithm. The legitimate UAV and spoofing attackers can always be authenticated by the different motion states. Performance analysis offered a comprehensive understanding of the proposed scheme. Extensive simulations confirm that the performance of the proposed scheme improves over 18% in resisting the intelligent spoofing UAV compared with the traditional methods.

Keywords UAV relay, physical layer authentication, mobility, manifold learning, diffusion map, state transition probability

Citation Xia S D, Tao X F, Li N, et al. Physical layer authentication in UAV-enabled relay networks based on manifold learning. Sci China Inf Sci, 2022, 65(12): 222302, https://doi.org/10.1007/s11432-021-3410-2

1 Introduction

The unmanned aerial vehicle (UAV) enabled relay network is a promising solution for throughput improvement and service range extension in further networks, especially adapting to the large-scale activity and disaster-fight [1, 2]. Equipped with specific wireless transceivers, the UAV relay can communicate with both ground users and base stations [3]. However, due to the openness of wireless channels, the identity information of the UAV relay can be easily wiretapped by the eavesdropper and further masqueraded by spoofing attackers [4–7]. The adversarial UAV can amplify and forward the falsified signals to the ground receivers, illegally tempering users' private information and causing enormous economic losses. Therefore, accurate UAV authentication is an essential prerequisite for UAV-enabled relay networks.

Currently, the secure access of wireless networks is provided by cryptography-based authentication protocols. The identities of the user and network are authenticated by key agreement and the inquiry request, e.g., the evolved packet system authentication and key agreement protocols (EPS-AKA) in the 4-th generation mobile networks (4G) [8], and the 5G-AKA protocols [9]. Although the effectiveness and reliability of AKA protocols have been confirmed in the terrestrial cellular network [9,10], it is difficult to apply them to the UAV relay directly. Firstly, the UAV relay is a resource-constrained device, which may not support the highly complex authentication protocols. Secondly, the UAV relay is usually fast-moving under the pre-designed trajectory, with a frequency handover with the ground devices. In this case, the

* Corresponding author (email: taoxf@bupt.edu.cn)

latency of authentication handover may cause the UAV to miss the best relay position, thus deteriorating the efficiency of UAV-enabled relay networks.

Physical layer security has been proposed as an alternative solution for secure wireless communications [11, 12]. Particularly, physical layer authentication (PLA) is a key complementary technique for secure access due to its robust security and low complexity [13–19]. The legitimate and spoofing signals are distinguished by comparing the physical layer attributes of received signals with the reference vector. Mathematically, PLA is to find a partition plane for the legitimate user and spoofer in physical layer attributes, such as received signal strength (RSS) [13, 14], channel impulse response (CIR) [15, 16], angle of arrival (AoA) [17], carrier frequency offsets (CFO) [18], Doppler frequency shift [19]. Physical layer attributes are time-varying as the wireless channel fading changes, presenting high randomness and spatiotemporal uniqueness. Therefore, PLA is difficult to be broken by spoofing attackers.

Some researchers have applied PLA to UAV authentication. The authors of [20] proposed a PLA scheme for the UAV relay using the generalized log-likelihood ratio test, where the parameters of received signals were estimated to judge the spoofing signals. In [21], a two-dimensional authentication factor was designed for PLA, which was constructed by combing the mean and variance of RSS. A cross-layer authentication scheme [22] was proposed based on PLA, where a fused decision program was derived by linear discriminant analysis to maximum separability of physical layer attributes. These studies provide implications for applying PLA to UAV authentication. However, they have not considered UAV mobility, whereas UAV usually flies with a pre-designed trajectory. These characteristics make the physical layer attributes present strong time-varying, limiting the application of the traditional PLA schemes.

On this basis, the authors of [23] proposed a PLA scheme for mobile UAVs based on trajectory prediction. The UAV relay was authenticated by comparing the predicted trajectory with the actual trajectory. The predicted and observed locations of the UAV were combined by a Kalman filter to enhance the authentication performance. It is a pioneering work to authenticate the UAV by combining the trajectory, which can guide the further design of the PAL. Nevertheless, since the communication of the UAV is usually burst, only authenticating the UAV trajectory cannot satisfy the time validity of authentication.

In this paper, we propose a real-time PLA scheme to authenticate the mobile UAV. The trajectory of the UAV is established by a Markov process, where the state transition matrix reflects UAV motion. According to the state transition probability, a neighborhood graph that contains K most likely transition state is constructed as the reference of a sample to perform PLA. Unlike [23], the proposed PLA scheme treats physical layer attributes as continuously changing states, where each state can be continuously authenticated by the state transition probability. Meanwhile, the state-of-the-art UAV-to-ground (U2G) channel is adopted in this paper to reflect the actual UAV scene according to [24, 25].

Although the time-varying nature of wireless channel fading provides robust security for PLA, it also causes poor reliability of PLA. In other words, because of the estimation error or the time-varying of the fading, physical layer attributes will significantly deviate from the reference at some time, leading to unreliable authentication results. Notably, UAV mobility would further aggravate this unreliability. If we continually use the traditional PLA for UAV relay, it becomes extremely difficult and resource-consuming to obtain a reference that accurately reflects the physical layer attributes of a legitimate UAV.

Recently, machine learning (ML) algorithms have been investigated to enhance the reliability of PLA. Essentially, ML algorithms act as the signal processing tools in PLA, which find the optimal partition plane for the legitimate user and spoofer in physical layer attributes, so as to relieve the influence of channel randomness on authentication [14–16, 26–28]. Specifically, an extreme learning machine-based PLA scheme was proposed in [26], where the attacking samples were artificially generated to find a more accurate segmentation plane for PLA. The authors of [27] systematically investigated the performance of decision tree (DT), support vector machine (SVM), and K-nearest-neighbors (KNN) based PLA scheme, where the classifiers were trained to counteract physical layer attribute fluctuations. The deep learning (DL) based PLA was proposed in [14–16], which derived a high-dimensional nonlinear presentation for physical layer attributes. A reliable PLA could be achieved since physical layer attributes for the legitimate users and attackers were always separable in the constructed feature space.

Nevertheless, the communication of the UAV-relay networks presents new characteristics compared with the traditional cellular network, leading to traditional PLA schemes being inapplicable. Firstly, due to the high mobility of the UAV relay, the value range of physical layer attributes for legitimate UAV and spoofer is largely overlapping. There is no linearly separable plane between the physical layer attributes of the legitimate UAV and the spoofing UAV. The trained partition plane by the traditional ML algorithm

could not effectively distinguish the time-varying physical layer attribute samples for legitimate UAV and spoofing UAV, leading to large errors in PLA decision [27]. Secondly, the supervised ML algorithms require a large number of training samples, which are difficult to obtain in UAV communication scenarios. The high-dimensional separable feature space for physical layer attributes is also difficult to train by the DL algorithm [16]. Therefore, it is urgent to explore new PLA architecture for UAV-relay networks.

Manifold learning is a promising solution to recognize nonlinearly separable physical layer data. It embeds high-dimensional data into low-dimensional manifold space based on the adjacency structure of data (or local topology changes of data) [29,30]. Even for nonlinearly separable physical layer data, it still can be distinguished by the different trends of data caused by different UAV trajectories. Meanwhile, the process of dimensionality reduction in manifold learning retains the main manifold of the physical layer data, i.e., the movement direction of UAV relay, whereas other minor manifold directions are discarded, i.e., the fluctuations of physical layer data caused by environment noise and estimation errors. Therefore, manifold learning further guarantees the reliability of PLA. Specifically, the authors of [15] proposed a kernel principal component analysis-based PLA scheme, where the physical layer data was projected into a potentially infinite-dimensional feature space to find a potential separable space. The study of [15] provided an insightful view to applying manifold leaning into PLA. However, without considering the nonlinear separability of physical layer attributes, it is difficult to apply to UAV authentication directly.

In this paper, we propose a diffusion map-based manifold learning algorithm to achieve the PLA for mobile UAV relay. A low-dimensional feature space is constructed based on the proposed diffusion map algorithm to represent the inherent manifold structure of physical layer attributes. Unlike [15], the connectivity of manifold structures is measured by the state transition probability instead of the distance between the samples. Therefore, the proposed PLA scheme can be adaptive to the arbitrary trajectories of UAVs. A Gaussian kernel function [30] is established to construct the pairwise adjacency matrix of the diffusion map. Motivated by [31, 32], the intrinsic dimension and the bandwidth of the kernel function are trained according to the correlation of samples. Finally, the nearest neighborhoods of a given sample are selected to construct the neighborhood graph as the reference values to perform PLA.

In a nutshell, the main contributions of this paper are summarized as follows.

• We propose a real-time PLA scheme to authenticate the mobile UAV based on the local correlation of physical layer attributes. The Markov process is established to reflect UAV motion characteristics, where the state transition probability measures the local correlation of physical layer attributes. The UAV relay can be continuously authenticated in real-time by treating physical layer attributes as a continuously changing state with a fixed correlation. The proposed scheme provides a feasible PLA framework to authenticate the moving terminals, which can be further extended to authenticate the moving terminals under arbitrary motion trajectories.

• We propose a diffusion map-based manifold learning algorithm and derive the inherent manifold structure of physical layer attributes, which overcomes the severe fluctuation of physical layer attributes caused by the time-varying fading and UAV mobility. A low-dimensional feature space is constructed based on the spectral embedding of the state transition matrix. Meanwhile, we build a neighborhood graph that contains K most likely transition states as the authentication reference. To our knowledge, this is the first work to achieve the PLA for mobile UAV relay using manifold learning, which provided a new feasible solution for recognizing nonlinearly separable physical layer data.

• We analyze the performance and complexity of the proposed PLA scheme to offer a comprehensive understanding of the proposed PLA scheme. Extensive simulations confirm that the proposed PLA scheme can achieve more than 18% performance improvement in resisting the intelligent spoofing UAV than the traditional DT, SVM, KNN, and DL-based PLA scheme.

The remainder of this paper is organized as follows. The system model is explained in Section 2. The proposed PLA scheme is described in Section 3. In Section 4, the implementation of the proposed diffusion map algorithm is illustrated. In Section 5, the performance analysis is investigated. Simulation results are provided in Section 6, and the conclusion and further work are drawn in Sections 7 and 8, respectively.

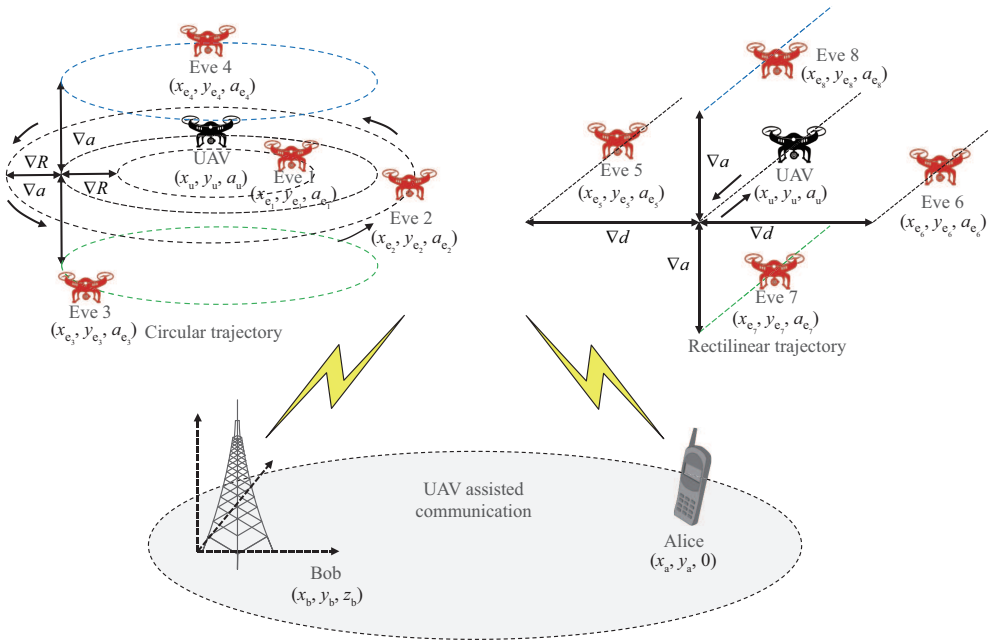

Figure 1 (Color online) UAV-enabled relay networks.

2 System model

2.1 Network model

Consider a scenario in which the ground user communicates with the ground base station (BS) through the UAV relay without a direct communication link. As commonly used in security-related studies, Alice, Bob, and Eve are used to represent the legitimate transmitter, the intended receiver, and the spoofing attackers, respectively. Eve masquerades as the legitimate UAV relay to amplify and forward the tampered signals to Bob when the legitimate UAV is idle. In other words, Eve sends the spoofing signals at the gap of legitimate signals to achieve its illegal purpose. The UAV relay and Eve fly with a pre-designed trajectory. All communication links are broadcast.

As shown in Figure 1, Alice and Bob are located at the three-dimensional (3D) coordinates of $\boldsymbol{\mathcal{L}}_{\mathrm{b}} = (0,0,0)$ and $\boldsymbol{\mathcal{L}}_{\mathrm{a}} = (x_{\mathrm{a}}, y_{\mathrm{a}}, 0)$, respectively. The trajectory of the UAV relay within each period T can be modeled as an N-length sequence. The location of the UAV at time slot t is given as

$$\boldsymbol{\mathcal{L}}_{\mathrm{u}}(t) = \left[x_{\mathrm{u}}(t), y_{\mathrm{u}}(t), a_{\mathrm{u}}(t)\right], \ t = 1, \ldots, N, \tag{1}$$

where $x_{\mathrm{u}}(t)$ and $y_{\mathrm{u}}(t)$ are the horizontal coordinates of the UAV relay, and $a_{\mathrm{u}}(t)$ denotes the altitude of the UAV relay. The trajectory of the UAV relay suffers the constraints as follows. Firstly, the UAV relay follows the same trajectory $\boldsymbol{\mathcal{L}}_{\mathrm{u}}(t)$ over consecutive periods until the re-planning process is triggered. Secondly, UAV needs to return to its original position by the end of each period T, which implies that the UAV trajectory is a closed curve in 3D space.

As shown in Figure 1, we consider the two most used UAV trajectories, i.e., circular trajectory [33] and rectilinear trajectory [34]. The circular trajectory of UAV can be modeled as

$$x_{\mathrm{u}}(t)^2 + y_{\mathrm{u}}(t)^2 = R_{\mathrm{u}}^2, \tag{2}$$

where R_{u} is the radius of the circular trajectory. The rectilinear trajectory of UAV is given as

$$y_{\mathrm{u}}(t) = k_{\mathrm{u}} x_{\mathrm{u}}(t) + C_{\mathrm{u}}, \tag{3}$$

where k_{u} and C_{u} are the direction and location of the rectilinear trajectory, respectively.

The location of Eve is defined as

$$\boldsymbol{\mathcal{L}}_{\mathrm{e}}(t) = \left[x_{\mathrm{e}}(t), y_{\mathrm{e}}(t), a_{\mathrm{e}}(t)\right]. \tag{4}$$

As confirmed in our previous studies [35,36], Eve has more probability of breaking through the PLA when its location is closer to the UAV relay. In this paper, we consider the intelligent Eve, whose trajectory is similar to that of the UAV relay. More specifically, intelligent Eve flies around the legitimate UAV at different horizontals or altitudes, which is the easiest area to break through PLA. Therefore, if the intelligent Eve can be authenticated, other attackers can also be authenticated. Note that we assume that the Eve is easily physically observed when its trajectory is the same as the legitimate UAV relay but in different locations, which is not the focus of this paper.

With the circular trajectory, two patterns of Eve are defined as follows.

Pattern 1. Eve has the same altitude as the UAV relay, like Eves 1 and 2, i.e., $a_{\mathrm{e}_1}(t) = a_{\mathrm{e}_2}(t) = a_{\mathrm{u}}(t)$, but has a different circular trajectory radius, which can be defined as

$$x_{\mathrm{e}_1}(t)^2 + y_{\mathrm{e}_1}(t)^2 = R_{\mathrm{e}_1}^2 = \left(R_{\mathrm{u}} - \nabla R\right)^2, \tag{5}$$

$$x_{\mathrm{e}_2}(t)^2 + y_{\mathrm{e}_2}(t)^2 = R_{\mathrm{e}_2}^2 = \left(R_{\mathrm{u}} + \nabla R\right)^2, \tag{6}$$

where ∇R is the constant trajectory radius difference between Eve and UAV relay.

Pattern 2. Eve has the same trajectory radius as the UAV relay, like Eve 3 and Eve 4, i.e., $R_{\mathrm{e}_3} = R_{\mathrm{e}_4} = R_{\mathrm{u}}$, but has a different altitude, which can be defined as

$$a_{\mathrm{e}_3}(t) = a_{\mathrm{u}}(t) - \nabla a, \tag{7}$$

$$a_{\mathrm{e}_4}(t) = a_{\mathrm{u}}(t) + \nabla a, \tag{8}$$

where ∇a is the constant altitude difference between Eve and UAV relay.

With the rectilinear trajectory, the other two patterns of Eve are defined as follows.

Pattern 3. Eve has the same altitude and direction as the UAV relay, like Eves 5 and 6, i.e., $a_{\mathrm{e}_5}(t) = a_{\mathrm{e}_6}(t) = a_{\mathrm{u}}(t)$ and $k_{\mathrm{e}_5} = k_{\mathrm{e}_6} = k_{\mathrm{u}}$, but is located at a different horizontal location, defined as

$$y_{\mathrm{e}_5}(t) = k_{\mathrm{e}_5} x_{\mathrm{e}_5}(t) + C_{\mathrm{e}_5} = k_{\mathrm{e}_5} x_{\mathrm{e}_5}(t) + \left(C_{\mathrm{u}} - \nabla d\right), \tag{9}$$

$$y_{\mathrm{e}_6}(t) = k_{\mathrm{e}_6} x_{\mathrm{e}_6}(t) + C_{\mathrm{e}_6} = k_{\mathrm{e}_6} x_{\mathrm{e}_6}(t) + \left(C_{\mathrm{u}} + \nabla d\right), \tag{10}$$

where ∇d is the constant horizontal location difference between Eve and UAV relay.

Pattern 4. Eve has the same horizontal trajectory as the UAV relay, like Eve 7 and Eve 8, i.e., $k_{\mathrm{e}_7} = k_{\mathrm{e}_8} = k_{\mathrm{u}}$ and $C_{\mathrm{e}_7} = C_{\mathrm{e}_8} = C_{\mathrm{u}}$, but is located at different altitudes, defined as

$$a_{\mathrm{e}_7}(t) = a_{\mathrm{u}}(t) - \nabla a, \tag{11}$$

$$a_{\mathrm{e}_8}(t) = a_{\mathrm{u}}(t) + \nabla a, \tag{12}$$

where ∇a is the constant altitude difference between Eve and UAV relay.

2.2 Channel model

Alice and UAV are assumed to be equipped with a single antenna, and Bob is equipped with m antennas. In the t-th time slot, Alice transmits the signal $s_{\mathrm{a}}(t)$. The received signal of the UAV relay is modeled as

$$r_{\mathrm{u}}(t) = \sqrt{P_{\mathrm{a}}} h_{\mathrm{au}}(t) s_{\mathrm{a}}(t) + N_{\mathrm{au}}, \tag{13}$$

where P_{a} is the transmitting power, h_{au} denotes the channel response of Alice to UAV (A2U) link, and $N_{\mathrm{au}} \sim \mathcal{CN}(0, \sigma_n^2)$ is the additional complex Gaussian noise. According to [24], h_{au} can be modeled by

$$h_{\mathrm{au}}(t) = L_{\mathrm{au}}(t) \cdot S_{\mathrm{au}}(t), \tag{14}$$

where $S_{\mathrm{au}}(t)$ denotes the Rayleigh fading coefficient that is modeled as a complex Gaussian variable with zero mean and unit variance, i.e., $S_{\mathrm{au}} \sim \mathcal{CN}(0, 1)$, and $L_{\mathrm{au}}(t)$ is the path loss. Since buildings may shade Alice, the A2U channel presents line-of-sight (LoS) and non-line-of-sight (NLoS) links at different time slots. According to [25], LoS and NLoS links possess different fading coefficients $L_{\mathrm{au}}(t)$, which can be expressed as

$$L_{\mathrm{au}}(t) = \begin{cases} \eta_{\mathrm{LoS}} \left(\dfrac{4\pi f_c d_{\mathrm{au}}(t)}{\mathrm{c}}\right)^{-\frac{\alpha}{2}}, & \text{LoS link}, \\ \eta_{\mathrm{NLoS}} \left(\dfrac{4\pi f_c d_{\mathrm{au}}(t)}{\mathrm{c}}\right)^{-\frac{\alpha}{2}}, & \text{NLoS link}, \end{cases} \tag{15}$$

where f_{c} (Hz) and c are the carrier frequency and speed of light, $d_{\mathrm{au}}(t) = \|\boldsymbol{\mathcal{L}}_{\mathrm{a}} - \boldsymbol{\mathcal{L}}_{\mathrm{u}}\|$ is the distance between UAV relay and Alice, $\|\cdot\|$ denotes the Euclidean norm, α denotes the path loss exponent, η_{LoS} and η_{NLoS} are the excessive losses for LoS and NLoS cases. The LoS probability is defined as P_{LoS}, which can be calculated as

$$P_{\mathrm{LoS}}(t) = \frac{1}{1 + Z\exp\left(-Q\left(\theta(t) - Z\right)\right)}, \tag{16}$$

where Z and Q are the environment-based constant values, $\theta(t) = 180/\pi \arcsin(a_{\mathrm{u}}(t)/d_{\mathrm{au}}(t))$. Accordingly, the NLoS probability is $P_{\mathrm{NLoS}} = 1 - P_{\mathrm{LoS}}$.

Then, the UAV relay amplifies and forwards $r_{\mathrm{u}}(t)$ to Bob, which can be designed as

$$s_{\mathrm{u}}(t) = G_{\mathrm{u}}(t) r_{\mathrm{u}}\left(t\right), \tag{17}$$

where $G_{\mathrm{u}}(t) = \sqrt{P_{\mathrm{u}}/\|r_{\mathrm{u}}(t)\|^2}$ is the amplification coefficient of the UAV relay [37], and P_{u} denotes the power of the UAV relay.

The received signals of Bob transmitted by the UAV relay can be modeled as

$$\boldsymbol{r}_{\mathrm{ub}}\left(t\right) = \boldsymbol{h}_{\mathrm{ub}}(t) s_{\mathrm{u}}\left(t\right) + \boldsymbol{N}_{\mathrm{ub}}, \tag{18}$$

where $\boldsymbol{h}_{\mathrm{ub}}(t) = [h_{\mathrm{ub}}^1(t), \ldots, h_{\mathrm{ub}}^M(t)]$ denotes the channel response of the UAV relay to Bob (U2B) link, $\boldsymbol{N}_{\mathrm{ub}} = [N_{\mathrm{ub}}^1(t), \ldots, N_{\mathrm{ub}}^M(t)]$ is the additional complex Gaussian noise, and $N_{\mathrm{ub}}^m \sim \mathcal{CN}(0, \sigma_n^2)$. Since the base station Bob is usually deployed in an open area, the U2B link always includes the LoS component. According to [25], $h_{\mathrm{ub}}^m(t)$ can be modeled as

$$h_{\mathrm{ub}}^m(t) = \eta_{\mathrm{LoS}} \left(\frac{4\pi f_{\mathrm{c}} d_{\mathrm{ub}}^m(t)}{\mathrm{c}}\right)^{-\frac{\alpha}{2}} S_{\mathrm{ub}}, \tag{19}$$

where $d_{\mathrm{ub}}^m(t)$ is the distance of the UAV relay to the m-th antenna of Bob, and S_{ub} denotes the Rayleigh fading, independently and identically distributed with S_{au}, i.e., $S_{\mathrm{ub}} \sim \mathcal{CN}(0, 1)$.

For attackers, the received signals of Eve transmitted by Alice can be modeled by

$$r_{\mathrm{e}}(t) = \sqrt{P_{\mathrm{a}}} h_{\mathrm{ae}}(t) s_{\mathrm{a}}(t) + N_{\mathrm{ae}}, \tag{20}$$

where $h_{\mathrm{ae}}(t)$ denotes the channel response of Alice to Eve (A2E) link that can be modeled by (14), and $N_{\mathrm{ae}} \sim \mathcal{CN}(0, \sigma_n^2)$ is the additional complex Gaussian noise. Then, Eve amplifies and forwards the falsified signals, defined as

$$s_{\mathrm{e}}(t) = \sqrt{P_{\mathrm{e}}} w_{\mathrm{e}}(t) \left(\sqrt{P_{\mathrm{e}}} h_{\mathrm{ae}}(t) \widetilde{s}_{\mathrm{a}}(t) + N_{\mathrm{ae}}\right), \tag{21}$$

where P_{e} is the transmitting power of Eve, $w_{\mathrm{e}}(t) = |r_{\mathrm{e}}(t)|^{-1}$, and $\widetilde{s}_{\mathrm{a}}(t)$ is the falsified $s_{\mathrm{a}}(t)$. The received signals of Bob transmitted by Eve can be modeled as

$$\boldsymbol{r}_{\mathrm{eb}}\left(t\right) = \boldsymbol{h}_{\mathrm{eb}}(t) s_{\mathrm{e}}(t) + \boldsymbol{N}_{\mathrm{eb}}, \tag{22}$$

where $\boldsymbol{h}_{\mathrm{eb}}(t)$ is the channel response of Eve to Bob, which can be modeled by (19), and $\boldsymbol{N}_{\mathrm{eb}}$ is the additional complex Gaussian noise with $N_{\mathrm{eb}}^m \sim \mathcal{CN}(0, \sigma_n^2)$.

In the following parts, given a signal without specifying the identity information, let $\boldsymbol{r}_b\left(t\right) = [r_{b1}(t), \ldots, r_{bM}(t)]$ denote the received signal of Bob.

3 The proposed PLA scheme for UAV relay

As shown in Figure 1, we consider a spoofing attacker Eve, who intends to masquerade the UAV relay and amplify and forward the tampered signals to access the network illegally. The main objective of Bob is to uniquely and unambiguously identify the transmitter by PLA. The basic idea is to use the local correlation of physical layer attributes of the received signals to distinguish the transmitters uniquely, detailed in Subsection 3.1. The main method is to design the identity indicator of the received signal based on the local correlation of physical layer attributes, detailed in Subsection 3.2.

3.1 The local correlation of physical layer attributes

In this paper, we consider a special physical layer attribute, i.e., the RSS, to realize PLA. The reasons can be summarized as follows. Firstly, RSS has a large value range compared with AoA, enabling it to have higher recognition accuracy for legitimate users and spoofing attackers. Secondly, RSS has greater randomness than CFO, which increases the difficulty of Eve to masquerade as the legitimate UAV successfully. Finally, the receiver can directly read RSS without the need for estimation like CSI, which is low complexity and easy to deploy. Since it is difficult for Eve to simultaneously infer multiple RSS of the received signal from a large search space, we construct the unique identity signature of the received signal by the combination of the RSS of M antennas as

$$\boldsymbol{I}(t) = \left[P_1(t), \ldots, P_M(t)\right], \tag{23}$$

where $P_m(t) = \|r_{bm}(t)\|^2$, $m = 1, \ldots, M$, represents the RSS of the m-th antenna at Bob.

The communication between Alice, UAV relay, and Bob includes two stages, i.e., the initial stage and the communication stage.

(1) The initial stage. Alice sends the access request signal through the UAV relay. Then, Bob calculates the RSS of received signals as the initial authentication reference as

$$\boldsymbol{R}(0) = \boldsymbol{I}(0). \tag{24}$$

We assume that Eve would not attack the initial stage. Because when Eve amplifies and forwards the access request signal, its signal would be superimposed with the legitimate signal, leading to a large signal power received by Bob. In this case, Eve can be easily detected by a power detector.

(2) The communication stage. Alice sends the legitimate signals to Bob by the UAV relay. While Eve amplifies and forwards the tampered signals in the gaps of legitimate signals to illegally access the network. In the t-th time slot, $\boldsymbol{I}(t)$ denotes the identity signature of the received signal.

Generally, the local correlation of physical layer attributes is defined as that communication links between special transceivers present similar physical layer attributes at the adjacent sampling time. Specifically, given a communication link with fixed transmitting power, the identity signature $\boldsymbol{I}(t)$ at the adjacent sampling time satisfies

$$||\boldsymbol{I}(t+1) - \boldsymbol{I}(t)|| < \xi, \tag{25}$$

where $\xi > 0$ represents the maximum difference of $\boldsymbol{I}(t)$ at adjacent sampling time. The larger sampling interval indicates the smaller correlation of physical layer attributes at adjacent sampling time.

To evaluate the correlation of physical layer attributes, the confidence coefficient is the most commonly used index, defined as the probability of RSS changing from $\boldsymbol{I}(t)$ to $\boldsymbol{I}(t+1)$, denoted by

$$\mathrm{con}(\boldsymbol{I}(t) \to \boldsymbol{I}(t+1)) = P\Big\{\boldsymbol{I}(t+1)|\boldsymbol{I}(t)\Big\}, \tag{26}$$

where $P\{\boldsymbol{I}(t+1)|\boldsymbol{I}(t)\}$ represents the conditional probability of $\boldsymbol{I}(t+1)$ given $\boldsymbol{I}(t)$. The larger $P(\boldsymbol{I}(t+1)|\boldsymbol{I}(t))$ indicates the stronger correlation of wireless channel at adjacent sampling time.

Let $\boldsymbol{I}_L(t)$ be the RSS of the legitimate UAV, and $\boldsymbol{I}_E(t)$ be the RSS of spoofing UAV. Given two adjacent RSS samples, the correlation of two consecutive legitimate RSS samples is much greater than that of the legitimate sample and attacking sample. In this case, the probability of RSS changing from a legitimate state to a legitimate state is much greater than that of a legitimate state to an attack state, denoted by

$$P(\boldsymbol{I}_L(t+1)|\boldsymbol{I}_L(t)) \gg P(\boldsymbol{I}_E(t+1)|\boldsymbol{I}_L(t)). \tag{27}$$

According to (27), the legitimate user and spoofing attacker can always be distinguished if the state transition probability (correlation) of RSS at adjacent sampling time can be estimated.

3.2 The proposed PLA scheme based on local correlation

The proposed authentication scheme is summarized in Figure 2. In this paper, the identity signatures of the received signals are modeled by a Markov chain, where each $\boldsymbol{I}(t)$ in the time domain is regarded as a state. The transition probability from state $t-1$ to state t can be defined as

$$p_{t,t-1} = \mathrm{con}(\boldsymbol{I}(t) \to \boldsymbol{I}(t+1)) = P\Big\{\boldsymbol{I}(t) \mid \boldsymbol{I}(t-1)\Big\}. \tag{28}$$

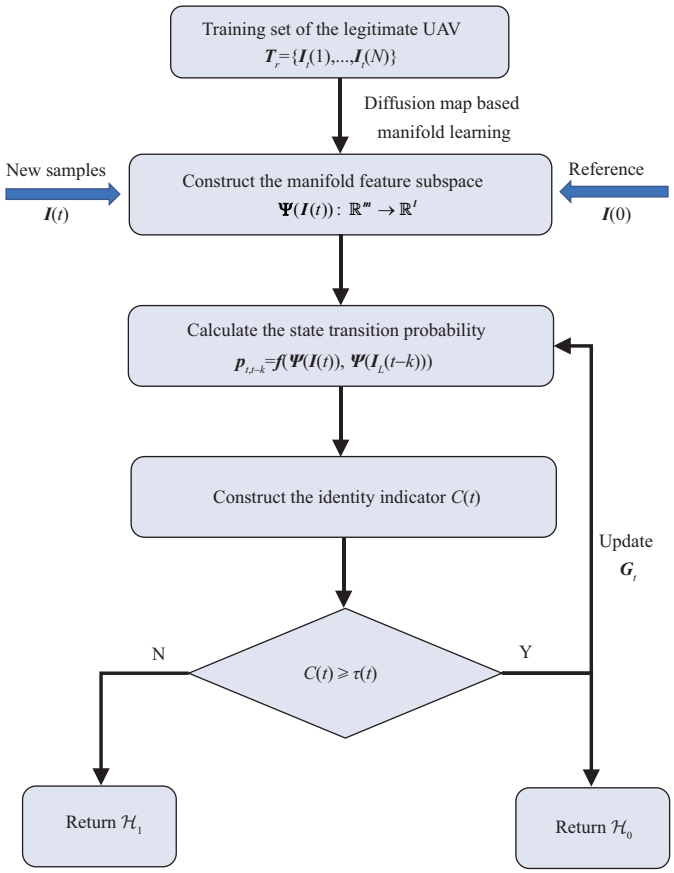

Figure 2 (Color online) Architecture of the proposed authentication scheme.

In [38], the transition probability of each state can be estimated by the expectation-maximization algorithm. However, in the time-varying channels of UAV, each $\boldsymbol{I}(t)$ is a variable with infinite possible values. It is difficult to estimate the transition probability of each state like [38]. Therefore, we investigate manifold learning to find a feature subspace that reflects the manifold structure of $\boldsymbol{I}(t)$ as

$$\Psi\left(\boldsymbol{I}(t)\right):\mathbb{R}^M\to\mathbb{R}^l, \tag{29}$$

where $l\leqslant M$ is the dimension of feature subspace. The detailed projection can be found in Section 4.

In the constructed feature subspace, the similarity of two samples is equivalent to the state transition probability as

$$f\Big(\Psi\big(\boldsymbol{I}(t)\big),\Psi\big(\boldsymbol{I}(t-1)\big)\Big)\triangleq p_{t,t-1}, \tag{30}$$

where $f(\cdot)$ is the function to measure the similarity of samples.

In this paper, we use the transition probability defined by (28) to authenticate the identity of $\boldsymbol{I}\left(t\right)$. Particularly, the transition probability from $\boldsymbol{I}_L(t-1)$ to $\boldsymbol{I}(t)$ is calculated as

$$p_{t,t-1}=f\Big(\Psi\left(\boldsymbol{I}(t)\right),\Psi\left(\boldsymbol{I}_L(t-1)\right)\Big), \tag{31}$$

where the subscript L represents the legitimate state. Then, a neighborhood graph $\boldsymbol{G}_t$ is established for $\boldsymbol{I}(t)$, which contains the previous K legitimate states as

$$\boldsymbol{G}_t=\left\{\boldsymbol{I}_L(t-1),\ldots,\boldsymbol{I}_L(t-K)\right\}. \tag{32}$$

According to the Markov property, the state transition probability in $\boldsymbol{G}_t$ is only related to the previous state defined as

$$p_{t-k,t-k-1}=f\Big(\Psi_L\left(\boldsymbol{I}(t-k)\right),\Psi\left(\boldsymbol{I}_L(t-k-1)\right)\Big), \tag{33}$$

where $k = 0, 1, \ldots, K$. Accordingly, the identity indicator of $\boldsymbol{I}(t)$ is defined as

$$C(t) = \begin{cases} p_{t,t-1}, & t = 1, \\ \dfrac{p_{t,t-1}}{p_{t-1,t-2}}, & 1 < t < K, \\ \dfrac{K p_{t,t-1}}{\sum_{k=1}^{K} p_{t-k,t-k-1}}, & t \geqslant K. \end{cases} \tag{34}$$

Finally, the PLA for UAV relay is modeled by binary hypothesis testing as

$$C(t) \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \tau(t), \tag{35}$$

where the null hypothesis $\mathcal{H}_0$ represents $\boldsymbol{I}(t)$ is authenticated as the legitimate signal, the alternative hypothesis $\mathcal{H}_1$ represents $\boldsymbol{I}(t)$ is authenticated as the attacker, and $\tau(t)$ is the decision threshold within the range of $(0, 1)$. The selection of $\tau(t)$ is detailed in Subsection 5.1.

The construction of $C(t)$ can be explained as follows. At the beginning of communication, i.e., $t = 1$, the identity indicator $C(t)$ is defined as the transition probability of $\boldsymbol{I}(t)$ from state $t-1$ to state t. However, due to the non-uniform sampling and the time-varying channel, $C(t)$ is a variable with large fluctuations, resulting in poor reliability and robustness of PLA. Therefore, as the communication continues, i.e., $1 < t < K$, $C(t)$ is defined as the ratio of the current $p_{t,t-1}$ to the previous $p_{t-1,t-2}$. In this case, the fluctuation of $C(t)$ can be mitigated to a certain extent. To further enhance the reliability of the PLA, when $t \geqslant K$, $C(t)$ is defined as the current $p_{t,t-1}$ ratio to the average state transition probability in neighborhood graph $\boldsymbol{G}(t)$. In this case, the fluctuation of $C(t)$ would be alleviated effectively. The detailed proof of $C(t)$ construction is given in Subsection 5.1.

4 Diffusion map based manifold learning

The manifold learning is a nonlinear mapping algorithm, which embeds one topological space inside another based on the adjacency structure of samples, aiming to recover a low-dimensional manifold embedded in a high-dimensional ambient space. In the process of dimensionality reduction, the local correlation of physical layer attributes is implicitly established by the paired adjacency matrix, which is further used in the design of PLA. Meanwhile, manifold learning recovers low-dimensional manifold structures from high-dimensional sampled data, which preserves the changes in physical layer attributes caused by UAV mobility, and relieves the influence of environmental noise and estimation error. Therefore, manifold learning is the key technology to achieve reliable UAV authentication.

In Subsection 4.1, the paired adjacency matrix is constructed by the kernel function to establish a Markov chain of the identity signatures. Then, a low-dimensional feature subspace is constructed to reflect the inherent manifold structure of identity signatures based on the proposed diffusion map detailed in Subsection 4.2. Finally, the bandwidth of the kernel function and the intrinsic dimension of the constructed feature subspace are selected to adapt to the specific manifold structure detailed in Subsection 4.3.

4.1 The paired adjacency matrix

The paired adjacency matrix establishes a Markov chain of identity signature samples [30], which seeks to preserve local structure in small neighborhoods on the manifold. The paired adjacency matrix is constructed based on the local topological structure over a graph of samples.

Specifically, the training set of the identity signatures for the UAV relay is given as

$$\boldsymbol{T}_r = \Big\{\boldsymbol{I}_t(1), \ldots, \boldsymbol{I}_t(N)\Big\}, \tag{36}$$

where the subscript t denotes the training sample and N is the number of training samples. For a fixed constant $\varepsilon > 0$, the neighborhoods of each training sample are defined as

$$\boldsymbol{I}_t(j) \in \boldsymbol{N}_i^{\varepsilon}, \quad \text{if } \|\boldsymbol{I}_t(i) - \boldsymbol{I}_t(j)\| < \varepsilon, \tag{37}$$

where $\boldsymbol{N}_i^{\varepsilon}$ is the neighbor set of $\boldsymbol{I}_t(i)$ with N_i samples.

To reflect the connectivity of training samples, the kernel function is adopted to measure similarity in which the larger kernel function represents two closer samples. In this paper, we define the connected matrix of $\boldsymbol{T}_r$ as $\boldsymbol{W} = (\omega_{ij}) \in \mathbb{R}^{N\times N}$, where each element of $\boldsymbol{W}$ is calculated as

$$\omega_{ij} = K\left(\boldsymbol{I}_t(i), \boldsymbol{I}_t(j)\right) = \begin{cases} \exp\left\{\dfrac{-\|\boldsymbol{I}_t(i) - \boldsymbol{I}_t(j)\|^2}{2\sigma^2}\right\}, & \boldsymbol{I}_t(j) \in \boldsymbol{N}_i^{\varepsilon}, \\ 0, & \text{otherwise}, \end{cases} \tag{38}$$

where $K(\cdot,\cdot)$ denotes the Gaussian kernel function, and σ indicates the Gaussian kernel bandwidth. Since the identity signatures of legitimate UAV and Eve are linear inseparable, the Gaussian kernel is adopted to measure the similarity.

According to [29], the training set $\boldsymbol{T}_r$ and the connected matrix $\boldsymbol{W}$ jointly determine the local geometry of identity signatures. Further, the connected matrix $\boldsymbol{W}$ is normalized as

$$\boldsymbol{P} = \boldsymbol{W}\boldsymbol{D}^{-1} = \left\{p_{ij}\right\}_{i,j=1}^{N} \in \mathbb{R}^{N\times N}, \tag{39}$$

where $\boldsymbol{D} = \mathrm{diag}\{d_1, \ldots, d_N\}$ is a diagonal matrix with $d_j = \sum_{i=1}^{N} \omega_{ij}$, and $p_{ij} = \omega_{ij} / \sum_{i=1}^{N} \omega_{ij}$, which satisfies $\sum_{i=1}^{N} p_{ij} = 1$. According to [30], p_{ij} can be interpreted as the transition probabilities from state $\boldsymbol{I}_t(j)$ to state $\boldsymbol{I}_t(i)$ in one time step. The larger p_{ij} is associated with nearby pairs of samples. Therefore, a Markov chain of identity signatures is established with the paired adjacency matrix $\boldsymbol{P}$.

4.2 The proposed diffusion map scheme

The basic idea of the diffusion map is to derive a low dimension feature subspace reflecting the manifold structure of identity signatures by an eigenanalysis of the state transition matrix of the Markov chain [29, 30]. The traditional diffusion map builds a manifold subspace and utilizes the diffusion distance to measure the similarity. Unlike the previous studies, we aim to construct a feature subspace that can measure the state transition probability.

To achieve this purpose, we propose a new diffusion map scheme, shown in Algorithm 1. Particularly, the constructed connected matrix $\boldsymbol{W}$ has the following characteristics. (1) Symmetry: $\boldsymbol{W} = \boldsymbol{W}^{\mathrm{T}}$. (2) Positive semi-definiteness: $\boldsymbol{v}^{\mathrm{T}}\boldsymbol{W}v \geqslant 0$, where $\boldsymbol{v}$ is the eigenvector of $\boldsymbol{W}$. (3) Non-negativity: $w_{ij} \geqslant 0$. In this case, $\boldsymbol{W}$ has real-valued eigenvalues with the orthogonal eigenvectors. The eigenvalue decomposition of $\boldsymbol{W}$ is defined as

$$\boldsymbol{W}\boldsymbol{v}_k = \lambda_k \boldsymbol{v}_k, \ k = 1, \ldots, N, \tag{40}$$

where λ_k is the k-th eigenvalue of $\boldsymbol{W}$ that satisfies $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_N \geqslant 0$. Then, $\boldsymbol{W}$ can be decomposed into

$$\boldsymbol{W} = \boldsymbol{V}\boldsymbol{\Lambda}\boldsymbol{V}^{\mathrm{T}}, \tag{41}$$

where $\boldsymbol{\Lambda} = \mathrm{diag}\left\{\lambda_1, \ldots, \lambda_N\right\}$ is a diagonal matrix, $\boldsymbol{V} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_N)$. Each element of $\boldsymbol{W}$ can be decomposed as

$$w_{ij} = \sum_{k=1}^{N} \lambda_k v_{ki} v_{kj} \approx \sum_{k=1}^{l} \lambda_k v_{ki} v_{kj}, \tag{42}$$

where v_{ki} and v_{kj} represent the k-th element of $\boldsymbol{v}_i$ and $\boldsymbol{v}_j$, respectively. In (42), the largest l eigenvalues and the corresponding eigenvectors can model p_{ij} accurately, while the remaining parts can be ignored as the noise. l denotes the intrinsic dimension, reflecting the minimum number of coordinates needed to represent the manifold.

In this paper, a new variant of the diffusion map scheme is proposed based on (42). Specifically, the projection for a sample $\boldsymbol{I}_t(i)$ can be calculated as

$$\Psi\left(\boldsymbol{I}_t(i)\right) = \left(\lambda_1^{1/2} v_{i1}, \ldots, \lambda_l^{1/2} v_{il}\right). \tag{43}$$

It can be seen that the inner product of two samples in the construed feature subspace is the function of the state transition probability p_{ij}, which is given as

$$\left\langle \Psi\left(\boldsymbol{I}_t(i)\right), \Psi\left(\boldsymbol{I}_t(j)\right) \right\rangle = \sum_{k=1}^{l} \lambda_k v_{ki} v_{kj} \approx d_j \cdot p_{ij}. \tag{44}$$

Algorithm 1 The proposed diffusion map algorithm

Input: $\boldsymbol{T}_r = \{\boldsymbol{I}_t(1), \ldots, \boldsymbol{I}_t(N)\}$, $\boldsymbol{I}(t)$;
Output: $\Psi(\boldsymbol{I}(t))$;
1: Select the neighborhoods of each training sample as $\boldsymbol{I}_t(i) \in \boldsymbol{N}_j^{\varepsilon}$, if $\|\boldsymbol{I}_t(i) - \boldsymbol{I}_t(j)\| < \varepsilon$;
2: Calculate paired adjacency matrix $\boldsymbol{W}$ as

$$\omega_{ij} = K(\boldsymbol{I}_t(i), \boldsymbol{I}_t(j)) = \begin{cases} \exp\left\{\dfrac{-\|\boldsymbol{I}_t(i) - \boldsymbol{I}_t(j)\|^2}{2\sigma^2}\right\}, & \boldsymbol{I}_t(i) \in \boldsymbol{N}_j^{\varepsilon}, \\ 0, & \text{otherwise}; \end{cases}$$

3: Conduct eigenvalue decomposition of $\boldsymbol{W}$ as $\boldsymbol{W}\boldsymbol{v}_k = \lambda_k \boldsymbol{v}_k$, $k = 1, \ldots, N$;
4: Given a new sample $\boldsymbol{I}(t)$, the projection is defined as

$$\Psi(\boldsymbol{I}(t)) = \left(\sum_{k=1}^{N} \frac{w_{tk} v_{k1}}{\lambda_1^{1/2}}, \ldots, \sum_{k=1}^{N} \frac{w_{tk} v_{kl}}{\lambda_l^{1/2}}\right).$$

Therefore, the similarity measurement in feature subspace can be designed as

$$f(\Psi(\boldsymbol{I}_t(i)), \Psi(\boldsymbol{I}_t(j))) = \frac{\langle \Psi(\boldsymbol{I}_t(i)), \Psi(\boldsymbol{I}_t(j)) \rangle}{d_j} = \frac{\sum_{k=1}^{l} \lambda_k v_{ki} v_{kj}}{d_j} \approx p_{ij}. \tag{45}$$

In this case, the similarity of samples in the constructed subspace approximates the state transition probability.

According to [30], a sample that is not originally included in the original ambient space can be projected into the feature subspace by weighting the coordinates of the kernel distance between the new point and the points in the original ambient space. Specifically, given a new identity signature $\boldsymbol{I}(t)$, the projection can be calculated as

$$\Psi(\boldsymbol{I}(t)) = \left(\sum_{k=1}^{N} \frac{w_{tk} v_{k1}}{\lambda_1^{1/2}}, \ldots, \sum_{k=1}^{N} \frac{w_{tk} v_{kl}}{\lambda_l^{1/2}}\right), \tag{46}$$

where w_{tk} can be calculated by (38). Therefore, a new feature subspace is constructed based on the proposed diffusion map, and the new samples can be projected into this subspace to conduct PLA.

4.3 Parameter selection

The performance of the proposed diffusion map scheme depends on the proper choice of bandwidth σ and the intrinsic dimension l. An appropriate σ and l should preserve the local connectivity of the manifold structure. Otherwise, if l is too large, the fluctuation of the sample set caused by noise still reserves. If l is too small, the underlying structure of the sample set would be dropped [39]. On the other hand, if σ is too small, the connectivity matrix cannot maintain the local geometry of the sample set accurately. Conversely, if σ is too large, the connectivity matrix may generate an excessively coarse description of the manifold structure [40].

In principle, the intrinsic dimension l is selected based on the training samples $\boldsymbol{T}_r$. According to [41], the training samples can be conceived as samples from high dimensional probability distributions defined on metric spaces. From a geometrical perspective, the intrinsic dimension estimation is to find a subset of the entire metric space that can be parameterized using a relatively small number of variables. Motivated by [42,43], since the RSS samples of UAV relay usually present the nonlinear data structure, the geometric (or fractal) method is suitable for estimating the intrinsic dimension.

Firstly, the correlation dimension is defined to measure the intrinsic dimension as

$$D = \lim_{\varepsilon \to 0} \frac{\ln \Omega(\varepsilon)}{\ln \varepsilon}, \tag{47}$$

where ε denotes the radius of the neighbors as similar with (37), and $\Omega(\varepsilon)$ denotes the correlation integral [41], which can be calculated as

$$\Omega(\varepsilon) = \frac{2}{N(N-1)} \sum_{i=1}^{N} \sum_{j=i+1}^{N} \mathcal{I}(\|\boldsymbol{I}_t(i) - \boldsymbol{I}_t(j)\| \leqslant \varepsilon), \tag{48}$$

where $\mathcal{I}(\cdot)$ is the indicator function, i.e., $\mathcal{I}(x) = 1$ if the condition x holds, otherwise $\mathcal{I}(x) = 0$. From the statistical view, $\Omega(\varepsilon)$ reflects the probability that a pair of samples' distance is less than or equal to ε.

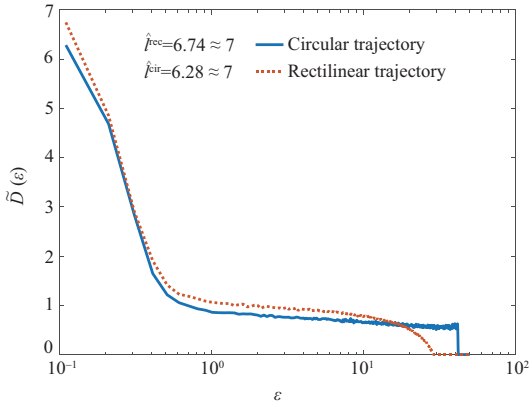

Figure 3 (Color online) Multiscale intrinsic dimension of $\tilde{D}(\varepsilon)$.

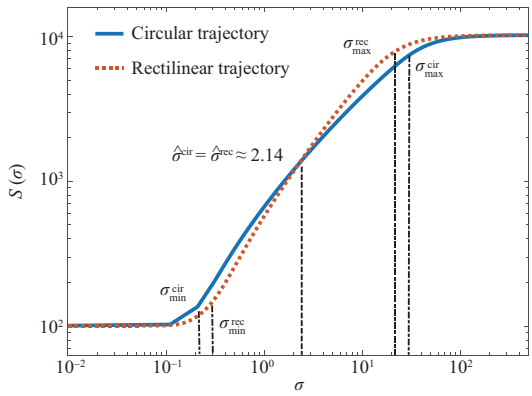

Figure 4 (Color online) Logarithmic plot of $S(\sigma)$ versus σ.

According to [42], the intrinsic dimension estimation is transformed to determine the best fit of the first linear region of the $\ln \Omega(\varepsilon)$ versus $\ln \varepsilon$ curve. To achieve this purpose, Ref. [41] suggested recasting the original definition of the correlation dimension in (47) to a multi-scale intrinsic dimension as

$$\hat{l} = \lim_{\varepsilon \to 0} \tilde{D}(\varepsilon) = \lim_{\varepsilon \to 0} \frac{\mathrm{d\ In}\ \Omega(\varepsilon)}{\mathrm{d\ In}\ \varepsilon} = \lim_{\varepsilon \to 0} \frac{\varepsilon}{\Omega(\varepsilon)} \frac{\mathrm{d}\ \Omega(\varepsilon)}{\mathrm{d}\ \varepsilon}, \tag{49}$$

where $\hat{l}$ is the estimated intrinsic dimension of the reconstructed subspace. As shown in Figure 3, the estimated intrinsic dimension is $\hat{l}^{\rm cir} = 6.28$ for the circular trajectory, while $\hat{l}^{\rm rec} = 6.74$ for the rectilinear trajectory. Since the intrinsic dimension must be an integer, we set $\hat{l}^{\rm cir} = \hat{l}^{\rm rec} \approx 7$ to avoid dropping the underlying structure of the sample set.

Motivated by [31, 40], the bandwidth σ can be estimated from the connected matrix $\boldsymbol{W}$. The basic idea is to compute the sum of non-zero elements in $\boldsymbol{W}$ for various values of σ and search for the range of values where the Gaussian bell shape is more pronounced.

Firstly, the sum of non-zero elements in $\boldsymbol{W}$ is calculated as

$$S(\sigma) = \sum_{i=1}^{N} \sum_{j=1}^{N} w_{ij}(\sigma), \tag{50}$$

where $w_{ij}(\sigma)$ is a function of σ defined by (38).

According to [44], the Gaussian bell shape would be more pronounced at the maximal linear range of the logarithmic plot of $S(\sigma)$. As shown in Figure 4, $\sigma_{\max}$ and $\sigma_{\min}$ represent the maximum and minimum of the maximal linear range of $L(\sigma)$, respectively. Then, we can get an estimation for σ as

$$\hat{\sigma} = \mathrm{In}\left(\frac{\sigma_{\max} + \sigma_{\min}}{2}\right), \tag{51}$$

where the estimated bandwidth for circular trajectory $\hat{\sigma}^{\rm cir}$ and rectilinear trajectory $\hat{\sigma}^{\rm rec}$ satisfies $\hat{\sigma}^{\rm cir} = \hat{\sigma}^{\rm rec} \approx 2.14$. Note that other methods also can estimate the intrinsic dimension [41] and the bandwidth [31], which can be studied as further work.

Combining Figure 3 with Figure 4, the parameters of the proposed diffusion map scheme would not change significantly as the change of the UAV trajectory. Therefore, the performance of the proposed authentication scheme is highly adaptable to the dynamic UAV trajectory.

Specifically, when the UAV hovers over a fixed location, the physical layer attributes of the UAV over a fixed location follow the same distribution. The current sample $\boldsymbol{I}(t)$ has a fixed correlation with the previous one $\boldsymbol{I}(t-1)$. The state transition probability $p_{t,t-1}$ can be regarded as a fixed value. In this case, PLA degrades into the typical static PLA problem, where the fluctuation of physical layer attributes caused by UAV motion can be ignored. The identity indicator $C(t)$ is a more stable value than moving UAV conditions, which also conforms to the test rules defined by (35). Therefore, the proposed authentication scheme can still work well when the UAV hovers over a fixed location.

Moreover, when the UAV flies in a random trajectory, not limited to the circular trajectory and rectilinear trajectory, the assumption of the local correlation for physical layer attributes is still valid. The current sample $\boldsymbol{I}(t)$ has a random correlation with the previous one $\boldsymbol{I}(t-1)$, in which the state transition probability $p_{t,t-1}$ can be regarded as a random value. In this case, the identity indicator $C(t)$ will fluctuate considerably, which may deteriorate the authentication performance. Therefore, the identity indicator $C(t)$ must be redesigned to improve authentication performance. This extension could be the next research in our further work.

5 Performance analysis

In this section, we analyze the authentication accuracy and the computational complexity of our proposed PLA scheme, respectively, in order to offer a comprehensive understanding of the proposed scheme.

5.1 Analysis of authentication accuracy

Since PLA is modeled by binary hypothesis testing, the false alarm rate $P_{\rm fa}$ and miss detection rate $P_{\rm md}$ are the most commonly used metrics to measure authentication accuracy [26–28]. Specifically, $P_{\rm fa}$ indicates the probability of the legitimate signals being falsely alarmed as the spoofing attack, and $P_{\rm md}$ denotes the probability of the spoofing signals being miss detected. The smaller $P_{\rm fa}$ and $P_{\rm md}$ indicate more accurate authentication.

According to (35), $P_{\rm fa}$ and $P_{\rm md}$ can be defined as

$$P_{\rm fa}(t) = P\{C(t) < \tau(t) \mid \mathcal{H}_0\}, \tag{52}$$

$$P_{\rm md}(t) = P\{C(t) > \tau(t) \mid \mathcal{H}_1\}, \tag{53}$$

where $C(t)$ and $\tau(t)$ indicate the decision statistic and decision threshold, respectively. The design of decision statistic $C(t)$ determines the ability of the proposed scheme to authenticate the legitimate UAV and the spoofing attacker. The decision threshold $\tau(t)$ should be selected to balance $P_{\rm fa}$ and $P_{\rm md}$. According to (52) and (53), a large $\tau(t)$ leads to a small $P_{\rm fa}$; i.e., a large $\tau(t)$ can reduce the probability that the legitimate signals are falsely authenticated. In contrast, a small $\tau(t)$ brings a small $P_{\rm md}$; i.e., a small $\tau(t)$ can reduce the probability that the spoofing signals are miss detected.

According to (34), the decision statistic $C(t)$ can be regarded as a function of $p_{t-k,t-k-1}$, $k = 0, 1, \ldots, K$. However, since $p_{t-k,t-k-1}$ is derived by the nonlinear mapping of the identity signatures, it is difficult to model $C(t)$ precisely. In the following part, we provide the simplified performance analysis for the proposed PLA scheme based on the constructed $C\,(t)$.

Case 1. When $t = 1$, by combining (39) with (45), $C(t)$ can be approximated to

$$C(t) = p_{t,t-1} = f(\Psi(\boldsymbol{I}(t)), \Psi(\boldsymbol{I}_L(t-1))) \approx \frac{\exp\left\{-\|\boldsymbol{I}(t) - \boldsymbol{I}_L(t-1)\|^2/2\sigma^2\right\}}{\sum_{\boldsymbol{I}_t(k)\in\boldsymbol{N}^{\varepsilon}_{t-1}} \exp\left\{-\|\boldsymbol{I}_L(t-1) - \boldsymbol{I}_t(k)\|^2/2\sigma^2\right\}}, \tag{54}$$

where $\boldsymbol{I}(t)$ denotes the current un-authenticated identity signature, $\boldsymbol{I}_L(t-1)$ indicates the previous legitimate identity signature, $\boldsymbol{N}^{\varepsilon}_{t-1}$ is the neighborhood set of $\boldsymbol{I}_L(t-1)$ constructed by the training set $\boldsymbol{T}_r$, and $\boldsymbol{I}_t(k)$ denotes the sample in $\boldsymbol{N}^{\varepsilon}_{t-1}$. It can be observed that the distribution of $C(t)$ is determined by $\boldsymbol{I}(t)$, $\boldsymbol{I}_L(t-1)$, and $\boldsymbol{N}^{\varepsilon}_{t-1}$ simultaneously.

Remark 1. If the training set $\boldsymbol{T}_r$ is enough and homogeneous distributed, $\boldsymbol{I}_L(t-1)$ can be equivalent to the mean of all the samples in its neighborhood set $\boldsymbol{N}^{\varepsilon}_{t-1}$. In this case, the denominator of $C(t)$, i.e., $S_{t-1} = \sum_{\boldsymbol{N}^{\varepsilon}_{t-1}} \exp\left\{-\|\boldsymbol{I}_L(t-1) - \boldsymbol{I}_t(k)\|^2/2\sigma^2\right\}$ can be approximate to a constant value. The authentication accuracy is directly related to the difference between $\boldsymbol{I}(t)$ and $\boldsymbol{I}_L(t-1)$.

Specifically, let $D^i_{t,t-1} = \|\boldsymbol{I}(t) - \boldsymbol{I}_L(t-1)\|^2$ represent the change of identity signatures in two adjacent sampling times, where $i = 0$ and 1 denote the condition of $\mathcal{H}_0$ and $\mathcal{H}_1$. According to (54), $C(t)$ negatively correlates with $D^i_{t,t-1}$. Therefore, if $D^0_{t,t-1} < D^1_{t,t-1}$, then $C(t)|\mathcal{H}_0 > C(t)|\mathcal{H}_1$ always satisfies. Nevertheless, the non-uniform sampling and time-varying channels will lead to large fluctuations in $D^i_{t,t-1}$, causing the condition of false alarm and miss detection.

Remark 2. If the communication mode and UAV trajectory are fixed, the difference of identity signatures in two adjacent sampling times is approximate to a constant, i.e., $D^i_{t,t-1} \approx C$. In this case, the authentication accuracy depends on the state of the training set.

Particularly, in the sparse region of the training set, the neighborhood set $\boldsymbol{N}^{\varepsilon}_{t-1}$ has few samples, where S_{t-1} would be a minor value. According to (54), a small denominator would cause a large $C(t)$. In this case, the spoofing signals are more likely to be undetected. While for the dense region of the training set, $\boldsymbol{N}^{\varepsilon}_{t-1}$ has a large number of samples, leading to a small value of $C(t)$. The legitimate signals intend to be falsely alarmed as attacking.

In conclusion, the value of $C(t)$ depends on the training sample state and sampling interval. Therefore, both non-uniform sampling and heterogeneous training samples make $C(t)$ fluctuate violently at different sampling times, resulting in poor authentication reliability and robustness. By combining Remarks 1 and 2, the threshold $\tau(t)$ should be selected in the range of $[\mathrm{e}^{-D^1_{t,t-1}/2\sigma^2}/S_{t-1}, \mathrm{e}^{-D^0_{t,t-1}/2\sigma^2}/S_{t-1}]$ to balance the P_{fa} and P_{md} according to the real application requirements.

Case 2. When $1 < t < K$, $C(t)$ can be approximated to

$$C(t) = \frac{p_{t,t-1}}{p_{t-1,t-2}} = \frac{f(\Psi(\boldsymbol{I}(t)), \Psi(\boldsymbol{I}_L(t-1)))}{f(\Psi(\boldsymbol{I}_L(t-1)), \Psi(\boldsymbol{I}_L(t-2)))} \approx \frac{S_{t-2}}{S_{t-1}} \cdot \exp\left\{-\frac{D^i_{t,t-1} - D^0_{t-1,t-2}}{2\sigma^2}\right\}. \tag{55}$$

Remark 3. The heterogeneous distribution of $\boldsymbol{T}_r$ is originated from the change of UAV velocity and trajectory. This change is usually slow and regular. Therefore, $\frac{S_{t-2}}{S_{t-1}}$ can be approximate to 1. In this case, the authentication accuracy depends on the difference between $D^i_{t,t-1}$ and $D^0_{t-1,t-2}$.

Let $X^i_{t,t-1} = D^i_{t,t-1} - D^0_{t-1,t-2}$. According to (55), $C(t)$ negatively correlates with $X^i_{t,t-1}$. Therefore, if $X^0_{t,t-1} < X^1_{t,t-1}$, then $C(t)|\mathcal{H}_0 > C(t)|\mathcal{H}_1$ always satisfies. Meanwhile, since $S_{t-2}/S_{t-1} \approx 1$, the effect of the heterogeneous training set on authentication can be reduced effectively.

Under the condition of uniform sampling and stable channel, the RSS changes of legitimate UAV at two adjacent sampling times are approximately equal. Therefore, $X^0_{t,t-1} \approx 0$ holds, thus $C(t)|\mathcal{H}_0 \approx 1$. However, under the case of non-uniform sampling with time-varying channels ($X^0_{t,t-1} \neq 0$), $C(t)$ still presents a large fluctuation, which still weakens the authentication reliability and robustness. In this case, the decision threshold $\tau(t)$ should be selected in the range of $[\mathrm{e}^{-X^1_{t,t-1}/2\sigma^2}, \mathrm{e}^{-X^0_{t,t-1}/2\sigma^2}]$.

Case 3. When $t \geqslant K$, $C(t)$ can be approximated to

$$\begin{aligned} C(t) &= \frac{K p_{t,t-1}}{\sum_{k=1}^{K} p_{t-k,t-k-1}} = \frac{K f(\Psi(\boldsymbol{I}(t)), \Psi(\boldsymbol{I}_L(t-1)))}{\sum_{k=1}^{K} f(\Psi(\boldsymbol{I}_L(t-k)), \Psi(\boldsymbol{I}_L(t-k-1)))} \\ &\approx \frac{1}{\frac{1}{K}\sum_{k=1}^{K} \frac{S_{t-k-1}}{S_{t-1}} \cdot \exp\left\{\frac{X^i_{t,t-k}}{2\sigma^2}\right\}}. \end{aligned} \tag{56}$$

Remark 4. Under the assumption of Remark 3, $\frac{S_{t-k-1}}{S_{t-1}} \approx 1$ holds. The authentication accuracy depends on the average of $\exp\{X^i_{t,t-k}/2\sigma^2\}$, $k = 1, \ldots, K$.

Let $Y^i_{t,t-k} = \exp\{X^i_{t,t-k}/2\sigma^2\}$ and $Z^i_t = \frac{1}{K}\sum_{k=1}^{K} Y^i_{t,t-k}$. According to (56), $C(t)$ negatively correlates with Z^i_t, which is equivalent to being negatively correlated with $Y^i_{t,t-k}$. Therefore, if $Y^0_{t,t-k} < Y^1_{t,t-k}$, then $Z^0_t < Z^1_t$, so that $C(t)|\mathcal{H}_0 > C(t)|\mathcal{H}_1$ always satisfies.

Under the condition of uniform sampling and stable channel, $Y^i_{t,t-k} \approx 1$ holds, thus $C(t)|H_0 \approx 1$. Meanwhile, under the non-uniform sampling with time-varying channels ($Y^0_{t,t-k} \neq 1$), let $\mathrm{Var}(Y^0_{t,t-k})$ be the variance of $Y^0_{t,t-k}$. According to the central limit theorem, the variance of Z^i_t can be indicated by $\frac{1}{K}\mathrm{Var}(Y^0_{t,t-k})$. In this case, the fluctuations in $C(t)$ caused by non-uniform sampling and time-varying channels can be alleviated effectively, thus greatly improving the authentication reliability and robustness. The decision threshold $\tau(t)$ should be selected in the range of $[1/Z^1_t, 1/Z^0_t]$.

5.2 Analysis of computational complexity

This subsection provides an analysis of the computational complexity of each process using time complexity as a function of the number of training samples N, the dimension of samples M, the intrinsic dimension l, the maximum sample size in the neighborhood set $T = \max\{N_i\}$, and other related factors if necessary.

Table 1 Simulation parameters

Parameter	Value
Transmission technology	OFDM
Number of subcarriers	52
Center frequency f_c	5.2 GHz
Bandwidth of each subcarrier	0.3125 MHz
Modulation mode	QPSK
Length of cyclic prefix	16 symbols
Noise power spectrum density	-174 dBm/Hz
Number of received antennas m	8
Sampling interval	3.2 μs
($P_{\rm a}$, $P_{\rm u}$, $P_{\rm e}$)	(100, 100, 100) mW
($\eta_{\rm LOS}$, $\eta_{\rm NLOS}$, α)	(3, 21, 4)
(Z, Q)	(11.95, 0.14)
(ε, K)	(5, 8)
(∇R, ∇a)	(7, 7)

The proposed PLA scheme includes two main processes. The one is the training process that obtains the low dimension manifold subspace using the proposed diffusion map algorithm. The other one is the authentication decision process based on the constructed manifold subspace.

The training process is composed of three steps. The first step is neighborhood selection, which is defined by (37). Given a sample $\boldsymbol{I}_t(i)$, the computing of $\|\boldsymbol{I}_t(i) - \boldsymbol{I}_t(j)\|$ needs $\mathcal{O}(NM)$ calculation, and sorting to get its neighborhood set takes $\mathcal{O}(NT)$. Therefore, for all N training samples, the time complexity of neighborhood selection is $\mathcal{O}(N^2(T+M))$. The second step is the calculation of the connected matrix $\boldsymbol{W} = (\omega_{ij}) \in \mathbb{R}^{N\times N}$ defined by (38), whose time complexity is $\mathcal{O}(NMT)$. Finally, the eigenvalue decomposition of $\boldsymbol{W}$ is carried out as (40). According to [45], since $\boldsymbol{W}$ is a very sparse matrix, i.e., each row or column contains only N_i non-zero elements, and N_i is usually small compared with N, the time complexity of eigenvalue decomposition for $\boldsymbol{W}$ is $\mathcal{O}((l+T)N^2)$. Therefore, the overall complexity of the training process is $\mathcal{O}((T+M+l)N^2)$.

The authentication decision process is comprised of three steps. The first step is the projection map of a new sample $\boldsymbol{I}\,(t)$ defined by (43), which has the time complexity of $\mathcal{O}(MNl)$. The second step is the similarity calculation for the current samples and the previous legitimate one given as (45). The time complexity of the inner product is $\mathcal{O}(l)$. Finally, the identity indicator $C(t)$ is calculated to conduct the authentication decision with the time complexity of $\mathcal{O}(1)$. Therefore, the overall complexity of the authentication decision process is $\mathcal{O}(MNl)$.

In conclusion, the proposed PLA scheme provided a low computational complexity, which can satisfy the time validity of UAV relay authentication.

6 Simulations

In this section, the performance of the proposed PLA scheme is simulated with the synthetic data set. The computer configurations are Intel(R) Xeon E5-1620 v2 CPU, 3.7 GHz basic frequency, 16 GB of DDR3-1600 RAM, and the simulation platform is MATLAB R2020b.

6.1 The generation of data set

The IEEE 802.11a WLAN communication system is adopted to construct the transmitting environment to reflect the UAV communication realistically. The baseband signals are randomly generated. Then, the $(2, 1, 7)$ convolution code is used for channel coding. The transmission of IEEE 802.11a is a multi-carrier modulation technology with orthogonal frequency division multiplexing (OFDM) [46]. The center frequency is 5.2 GHz with 52 subcarriers. The bandwidth of each subcarrier is 0.3125 MHz, and the total bandwidth is 20 MHz. Each OFDM symbol is modulated by the quadrature phase shift keying (QPSK). The three stages m-sequence is used to spread the spectrum. The cyclic prefix is 16 symbols, and the length of fast Fourier transform (FFT) is 64. The channel matrix is generated according to (14) and (19). The number of received antennas of Bob is set to 8, where the antenna interval is 0.25 m. The noise power spectral density is -174 dBm/Hz. The detailed parameters are summarized in Table 1.

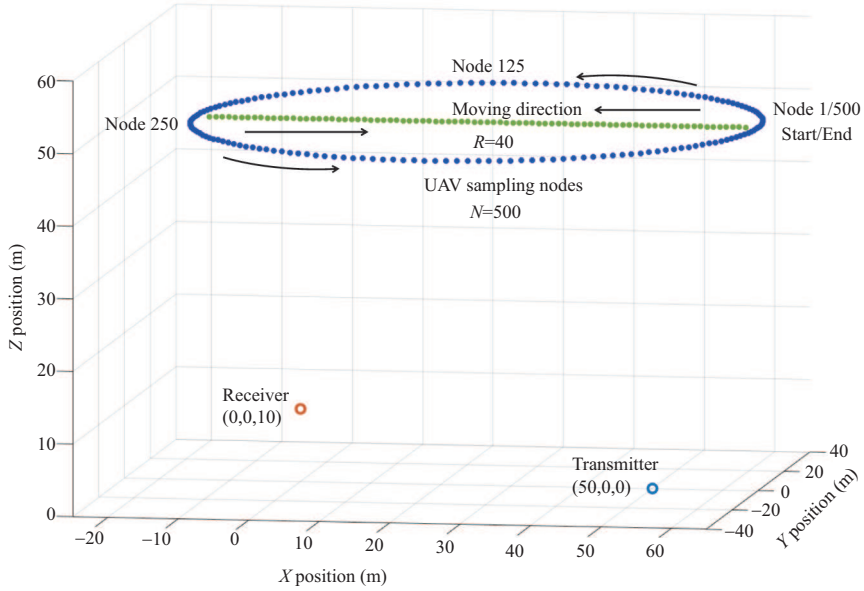

Figure 5 (Color online) Position of all nodes in simulations.

Figure 5 provides the positions of all nodes in the simulations. Particularly, the transmitter Alice is located at position $(50, 0, 0)$ m. The receiver Bob is located at the position $(0, 0, 10)$ m. The legitimate UAV is flying over the transceivers with the altitude of $a_{\mathrm{u}}(t) = 50$ m. For the circular trajectory, the circle center is $(25, 0, 50)$ m, and the radius is $R = 40$ m. While for rectilinear trajectory, the UAV flies in the direction of the connection of the transceivers. There are $N = 500$ sampling nodes on the trajectory of UAV, where the receiver collects one data frame at each sampling node. One data frame contains 8 OFDM symbols, and the average symbolic power is used as the RSS of the received signals. The intervals between adjacent sampling nodes are $\nabla S = \|\boldsymbol{\mathcal{L}}(t) - \boldsymbol{\mathcal{L}}(t-1)\| = 0.5$ m. The spoofing UAV (Eve) flies around the legitimate UAV with $\nabla R = \nabla d = \nabla a = 10$ m. Eve sends spoofing signals with the same transmitting power of a legitimate UAV (i.e., $P_{\mathrm{e}} = P_{\mathrm{u}} = 100$ mW) in the absence of the legitimate signals. Without a special declaration, we set the odd sampling nodes are the legitimate samples, and other nodes are spoofing samples.

Figure 6 presents the sampling space of the identity signatures under different sampling nodes. As can be seen, the RSS samples of the legitimate UAV have an inevitable overlap with Eve's samples. Different from traditional static communication scenarios, there is a large probability that two UAVs moving at high speed have similar channels with the receiver at certain sampling times. Therefore, it is difficult to find a partition plane for spoofing samples and legitimate samples, limiting the application of traditional classifier-based authentication schemes, such as DT, SVM, KNN, and DL-based schemes [16, 27]. Nonetheless, as shown in Figure 6, the spoofing samples are different from the legitimate samples at different sampling nodes, providing the opportunity to achieve the PLA. Meanwhile, it can be seen from Figure 6(b) that the samples of Eves 5 and 6 are always close to the legitimate samples. The authentication of Eves 5 and 6 is a difficulty in this paper. Moreover, because of the effect of UAV trajectory, the identity signature samples are not uniformly distributed. Particularly, the samples in nodes 1–50, 450–500, and 225–275 present dense distribution for circular trajectory. However, the samples in nodes 50–225 and 275–450 are sparse. For rectilinear trajectory, the samples in nodes 160–340 are dense, while other sampling nodes are sparse.

6.2 Simulations and analysis

As shown in Table 2, the authentication results in the statistical test can be summarized as true legitimacy (TL), false alarm (FA), miss detection (MD), and true attack (TA). Specifically, the TL represents the case where the legitimate signal is correctly authenticated. Otherwise, if the legitimate signal is misidentified as an attack, it is called an FA. Likewise, the TA indicates the case where the spoofing signal is authenticated successfully. And the situation in which the spoofing signals are authenticated as legitimate is called an MD. Given an unknown signal, the authentication result of this signal can only be one of the above four

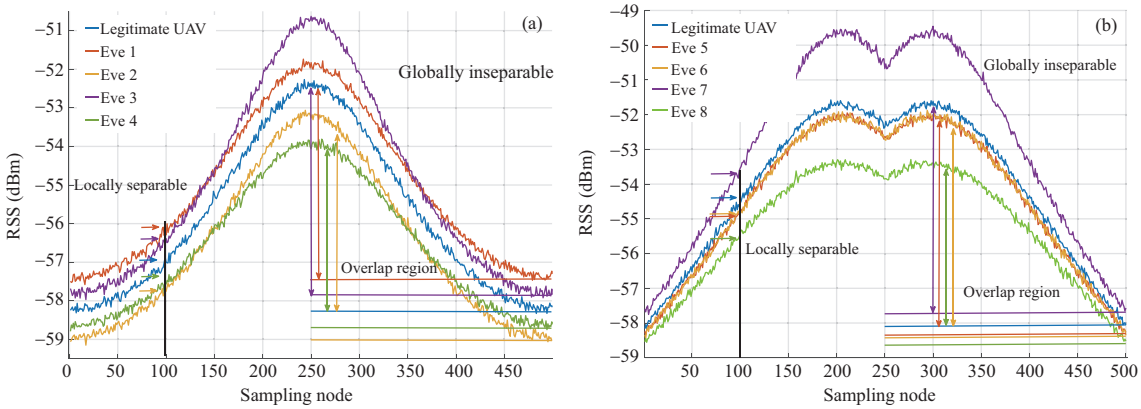

Figure 6 (Color online) Sampling space of the identity signatures. (a) Circular trajectory; (b) rectilinear trajectory.

Table 2 The definition of authentication results

Predicted	Actual	
	Legitimacy	Attack
Legitimacy	TL	MD
Attack	FA	TA

results. According to (52) and (53), the false alarm rate and miss detection rate can be calculated as

$$P_{\rm fa} = \frac{\rm FA}{\rm TL + FA}, \tag{57}$$

$$P_{\rm md} = \frac{\rm MD}{\rm TA + MD}, \tag{58}$$

where $P_{\rm fa}$ denotes the ratio of the false alarm number to the total actual legitimacy number, and $P_{\rm md}$ indicates the ratio of the miss detection number to the total actual attack number.

Figure 7 provides the performance of the proposed authentication scheme at the different sampling nodes. As shown in Figure 7(a), $P_{\rm fa}$ and $P_{\rm md}$ are always less than 0.01 under the circular trajectory, confirming that the proposed scheme can effectively authenticate the legitimate UAV and attackers. Meanwhile, $P_{\rm fa}$ performs poorly at the sparse region of training data, namely nodes 50–225 and 275–450, while $P_{\rm fa}$ performs well at the dense regions, i.e., nodes 1–50, 225–275, and 450–500. This indicates that sufficient training samples can guarantee the ability of the proposed scheme to authenticate the legitimate UAV. From another perspective, it can be seen that $P_{\rm md}$ decreases as increase of the difference of $\boldsymbol{I}(t)$ at adjacent sampling nodes, namely $D^1_{t,t-1}$. Specifically, $P_{\rm md}$ of Eves 1 and 2 increases from node 1 to 250, and decreases from node 250 to 500, because the $D^1_{t,t-1}$ of Eves 1 and 2 increases from node 1 to 250 and decreases from node 250 to 500. While the $P_{\rm md}$ of Eve 3 and Eve 4 has the reverse trend. Therefore, the attackers are more easily authenticated as $D^1_{t,t-1}$ increases. As shown in Figure 7(b), the performance of the proposed scheme under rectilinear trajectory presents same trend with circular trajectory. That is, $P_{\rm fa}$ presents a better performance at the dense region, i.e., node 160 to 340, while $P_{\rm md}$ presents better performance as $D^1_{t,t-1}$ increases, i.e., node 150 to 400. Meanwhile, for Eves 5 and 6, $P_{\rm md}$ is a high value at node 0–50, and node 450–500. Because $D^1_{t,t-1} \approx D^0_{t,t-1}$ holds at these sampling nodes, the proposed authentication scheme cannot distinguish the legitimate signals and spoofing signals. Particularly, in the near region of node 250, $P_{\rm fa}$ and $P_{\rm md}$ have a certain increase. Because the density of training samples changes greatly before and after this node shown in Figure 6, $C(t)$ has a large fluctuation, leading to the signals being more likely to be incorrectly authenticated.

Figure 8 provides the false alarm rate $P_{\rm fa}$ versus the number of training samples N under different sampling intervals ∇S, where the threshold is set to guarantee $P_{\rm md}$ less than 0.01. As can be seen, $P_{\rm fa}$ would decrease as the number of training samples increases until the converges when the training samples are greater than 500. Meanwhile, $P_{\rm fa}$ of legitimate UAV with the circular trajectory outperforms that of the rectilinear trajectory. This is because the identity signature in the circular trajectory presents a denser distribution compared with the rectilinear trajectory, which confirms the solution of Remark 2. From another perspective, Figure 8 indicates that $P_{\rm fa}$ increases with the increase of ∇S. By combining

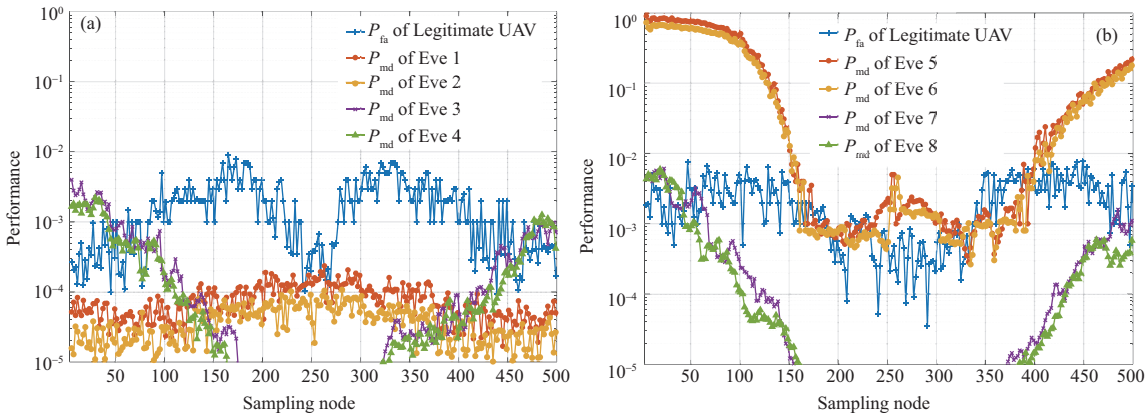

Figure 7 (Color online) Performance of the proposed PLA scheme at different sampling nodes. (a) Circular trajectory; (b) rectilinear trajectory.

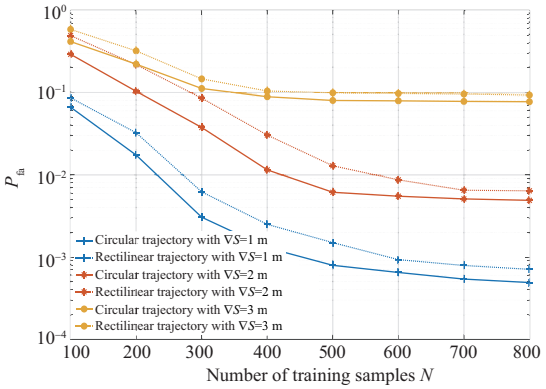

Figure 8 (Color online) False alarm rate versus training samples quantity.

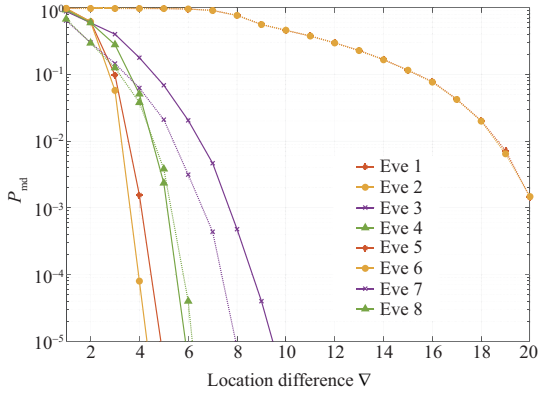

Figure 9 (Color online) Miss detection rate versus the location difference.

(54)–(56), $|C(t)|\mathcal{H}_0 - C(t)|\mathcal{H}_1|$ would decrease as the increase of sampling interval ∇S. To guarantee the miss detection rate, the large threshold selection leads the legitimate signals to be more likely to be falsely authenticated, i.e., a large $P_{\rm fa}$. Therefore, once the legitimate UAV keeps silent in a period, the authentication performance of new communications would deteriorate. For the application with robust security requirements, the proposed authentication process needs to be rebuilt periodically.

Figure 9 analyzes the miss detection rate $P_{\rm md}$ versus the location difference between Eve and UAV relay ∇, which is defined as $\nabla = \nabla a = \nabla R$. The threshold is selected to guarantee the $P_{\rm md}$ less than 0.01. As can be seen, $P_{\rm md}$ decreases as ∇ increases. According to (15) and (19), the difference in identity signatures between legitimate UAV and Eve, namely $D^1_{t,t-1}$, is positively correlated with ∇. Therefore, $C(t)|\mathcal{H}_1$ would decrease as the increase of ∇. Given a fixed communication mode of legitimate UAV, i.e., $C(t)|\mathcal{H}_0$, is a relatively stable value, the smaller $C(t)|\mathcal{H}_1$ indicates that the spoofing attackers are more likely to be authenticated correctly, leading to a smaller $P_{\rm md}$. Meanwhile, we observe that ∇ has different effects on different attack patterns. Particularly, the samples of Eves 5 and 6 are the most difficult to be authenticated correctly. Figure 6(b) shows that the identity signatures of Eves 5 and 6 present the most similar with legitimate samples, causing a large $P_{\rm md}$. Therefore, we can conclude the circular trajectory of UAV presents better performance to resist spoofing attacks than that of the rectilinear trajectory.

Figure 10 provides the receiver operating characteristic (ROC) curve to compare the proposed authentication scheme with other ML-based PLA schemes, i.e., the DT, SVM, KNN, and DL-based PLA. We select the most difficult authenticated attackers, namely Eve 5, with the number of training samples $N = 500$, the sampling interval of legitimate UAV $\nabla S = 1$ m, and the location difference $\nabla = 10$ m. It can be seen that the area under curve (AUC) of the proposed scheme is more than 18% larger than that of other schemes under the worst performance, indicating that the proposed scheme outperforms other schemes. Nevertheless, Figure 6 indicates that the identity signatures of different sampling nodes present

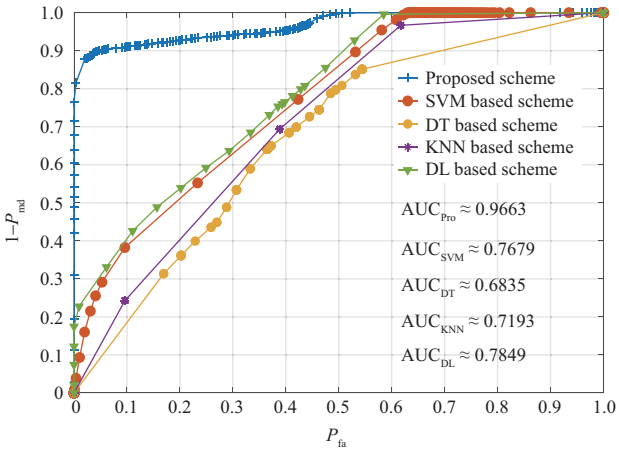

Figure 10 (Color online) Receiver operating characteristic curve.

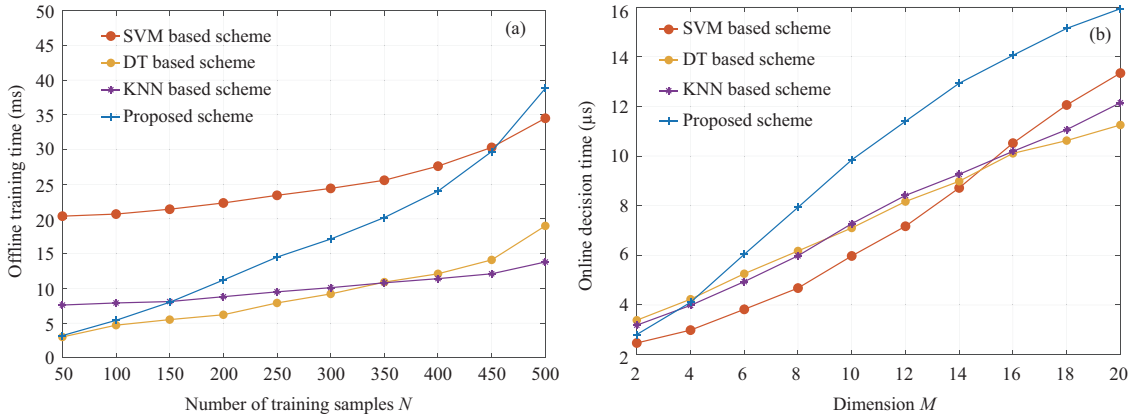

Figure 11 (Color online) The computational time of the proposed PLA scheme and the benchmark solutions. (a) Offline training time with $M = 8$; (b) online decision time with $N = 500$.

different values. By adding the sampling serial number to the identity signatures, the DT, SVM, KNN, and DL-based authentication scheme can separate the legitimate signal from the spoofing signals. However, this method also brings new security problems; e.g., the attacker can also forge the serial number to masquerade legitimate users. The serial number is an artificial endowed value instead of the objective physical layer attributes, which is more easily forged. Therefore, we can conclude that our proposed PLA scheme is more accurate for authenticating the moving UAV relay than the existing benchmark solutions.

Figure 11 compares the complexity of the proposed scheme with the benchmark solutions using computational time. Because the DL algorithm [16] is much more complex than other algorithms, it is not considered in the comparison. Figure 11(a) compares the proposed scheme with benchmark solutions using offline training time, which represents the preparation time before PLA. As can be seen, the training time of the proposed scheme is between the SVM and DT algorithm when $N \leqslant 450$, and larger than the SVM algorithm when $N = 500$. In combination with Figure 8, the performance of the proposed mechanism converges at $N = 500$. Therefore, the proposed scheme greatly improves the performance of UAV authentication with a slight increase in the complexity of the training process. Figure 11(b) compares the online decision time of the proposed scheme with the benchmark solutions, which is directly related to the real-time authentication latency. As can be seen, although the online decision time of the proposed PLA scheme is slightly larger than other benchmark solutions, the calculation time has reached the microsecond level, which is less than 16 ms. Meanwhile, we observe that the growth trend of the proposed scheme is similar to other benchmark solutions. Therefore, we can conclude that the proposed scheme is suitable for latency-sensitive applications.

7 Conclusion

In this paper, we proposed a mobile PLA scheme, based on manifold learning, for the UAV-enabled relay networks. This was the first work to realize the real-time PLA for mobile UAV relay by establishing the Markov chain of physical layer identity signatures. To achieve the separation of non-linear physical layer data in mobile PLA, we constructed a manifold feature space by the proposed diffusion map algorithm to reflect the state transition probability of identity signatures. Then, we established the local correlation of the Markov chain as the test statistic of received signals. The effect of training sample density, sampling interval, and the attack location on the authentication performance was depicted to offer a comprehensive understanding of the proposed scheme. Extensive simulations were conducted, which confirmed that the proposed scheme could effectively resist the spoofing UAV attack under the mobile scenarios, where the performance outperformed other schemes more than 18% in extremely worse cases. The proposed scheme provided a feasible framework to authenticate the mobile terminal, which can be further extended to authenticate the moving terminals under arbitrary motion trajectories.

8 Further work

With the popularity of massive multiple-input-multiple-output (MIMO) technology, the communication capacity is greatly improved, which provides rich spatial freedom for transmission. Considering the multi-path channel would offer more observations for the receiver, physical layer authentication schemes based on MIMO technology would further provide security enhancement.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61932005, 61941105), Shenzhen Science and Technology Innovation Commission Free Exploring Basic Research Project (Grant No. 2021Szvup008), and 111 Project of China (Grant No. B16006).

References

1 Wang H, Zhao H, Zhang J, et al. Survey on unmanned aerial vehicle networks: a cyber physical system perspective. IEEE Commun Surv Tut, 2020, 22: 1027–1070
2 Li B, Fei Z, Zhang Y. UAV communications for 5G and beyond: recent advances and future trends. IEEE Internet Things J, 2019, 6: 2241–2263
3 Shi W, Li J, Cheng N, et al. Multi-drone 3-D trajectory planning and scheduling in drone-assisted radio access networks. IEEE Trans Veh Technol, 2019, 68: 8145–8158
4 Sun X, Ng D W K, Ding Z, et al. Physical layer security in UAV systems: challenges and opportunities. IEEE Wireless Commun, 2019, 26: 40–47
5 You X H, Wang C-X, Huang J, et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci China Inf Sci, 2021, 64: 110301
6 Guo Y, Wu M, Tang K, et al. Covert spoofing algorithm of UAV based on GPS/INS-integrated navigation. IEEE Trans Veh Technol, 2019, 68: 6557–6564
7 Li B, Fei Z, Zhang Y, et al. Secure UAV communication networks over 5G. IEEE Wireless Commun, 2019, 26: 114–120
8 Bikos A N, Sklavos N. LTE/SAE security issues on 4G wireless networks. IEEE Secur Privacy, 2013, 11: 55–62
9 Jiang L, Chang X, Bai J, et al. Dependability analysis of 5G-AKA authentication service from server and user perspectives. IEEE Access, 2020, 8: 89562–89574
10 Zhang M X, Fang Y. Security analysis and enhancements of 3GPP authentication and key agreement protocol. IEEE Trans Wireless Commun, 2005, 4: 734–742
11 Wang H M, Zhang X, Jiang J C. UAV-involved wireless physical-layer secure communications: overview and research directions. IEEE Wireless Commun, 2019, 26: 32–39
12 Wang H M, Zhang X. UAV SECURE DOWNlink NOMA transmissions: a secure users oriented perspective. IEEE Trans Commun, 2020, 68: 5732–5746
13 Ji X S, Huang K Z, Jin L, et al. Overview of 5G security technology. Sci China Inf Sci, 2018, 61: 081301
14 Xiao L, Wan X, Han Z. PHY-layer authentication with multiple landmarks with reduced overhead. IEEE Trans Wireless Commun, 2018, 17: 1676–1687
15 Fang H, Wang X, Hanzo L. Learning-aided physical layer authentication as an intelligent process. IEEE Trans Commun, 2019, 67: 2260–2273
16 Liao R F, Wen H, Chen S, et al. Multiuser physical layer authentication in Internet of Things with data augmentation. IEEE Internet Things J, 2020, 7: 2077–2088
17 Abdelaziz A, Burton R, Barickman F, et al. Enhanced authentication based on angle of signal arrivals. IEEE Trans Veh Technol, 2019, 68: 4602–4614
18 Hou W, Wang X, Chouinard J Y, et al. Physical layer authentication for mobile systems with time-varying carrier frequency offsets. IEEE Trans Commun, 2014, 62: 1658–1667
19 Fu Q Y, Feng Y H, Wang H M, et al. Initial satellite access authentication based on Doppler frequency shift. IEEE Wireless Commun Lett, 2021, 10: 498–502
20 Huang K W, Wang H M. Combating the control signal spoofing attack in UAV systems. IEEE Trans Veh Technol, 2018, 67: 7769–7773
21 Hoang T M, Nguyen N M, Duong T Q. Detection of eavesdropping attack in UAV-aided wireless systems: unsupervised learning with one-class SVM and k-means clustering. IEEE Wireless Commun Lett, 2020, 9: 139–142

22 Wang H, Fang H, Wang X. Safeguarding cluster heads in UAV swarm using edge intelligence: linear discriminant analysis-based cross-layer authentication. IEEE Open J Commun Soc, 2021, 2: 1298–1309
23 Jiang C, Fang Y, Zhao P, et al. Intelligent UAV identity authentication and safety supervision based on behavior modeling and prediction. IEEE Trans Ind Inf, 2020, 16: 6652–6662
24 Wang H M, Zhang Y, Zhang X, et al. Secrecy and covert communications against UAV surveillance via multi-hop networks. IEEE Trans Commun, 2020, 68: 389–401
25 Song Q H, Zeng Y, Xu J, et al. A survey of prototype and experiment for UAV communications. Sci China Inf Sci, 2021, 64: 140301
26 Wang N, Jiang T, Lv S, et al. Physical-layer authentication based on extreme learning machine. IEEE Commun Lett, 2017, 21: 1557–1560
27 Pan F, Pang Z, Wen H, et al. Threshold-free physical layer authentication based on machine learning for industrial wireless CPS. IEEE Trans Ind Inf, 2019, 15: 6481–6491
28 Qiu X, Jiang T, Wu S, et al. Physical layer authentication enhancement using a Gaussian mixture model. IEEE Access, 2018, 6: 53583–53592
29 Ma Y, Fu Y. Manifold Learning Theory and Applications. Boca Raton: CRC Press, 2012
30 Olson C C, Judd K P, Nichols J M. Manifold learning techniques for unsupervised anomaly detection. Expert Syst Appl, 2018, 91: 374–385
31 Lindenbaum O, Salhov M, Yeredor A, et al. Gaussian bandwidth selection for manifold learning and classification. Data Min Knowl Disc, 2020, 34: 1676–1712
32 Mishne G, Cohen I. Multiscale anomaly detection using diffusion maps. IEEE J Sel Top Signal Process, 2013, 7: 111–123
33 Song Q, Zheng F C, Zeng Y, et al. Joint beamforming and power allocation for UAV-enabled full-duplex relay. IEEE Trans Veh Technol, 2019, 68: 1657–1671
34 Zeng Y, Zhang R, Lim T J. Throughput maximization for UAV-enabled mobile relaying systems. IEEE Trans Commun, 2016, 64: 4983–4996
35 Li N, Xia S D, Tao X F, et al. An area based physical layer authentication framework to detect spoofing attacks. Sci China Inf Sci, 2020, 63: 222302
36 Xia S, Tao X, Li N, et al. Multiple correlated attributes based physical layer authentication in wireless networks. IEEE Trans Veh Technol, 2021, 70: 1673–1687
37 Zhang S, Zhang H, He Q, et al. Joint trajectory and power optimization for UAV relay networks. IEEE Commun Lett, 2018, 22: 161–164
38 He X F, Dai H Y, Ning P. HMM-based malicious user detection for robust collaborative spectrum sensing. IEEE J Sel Areas Commun, 2013, 31: 2196–2208
39 Camastra F, Staiano A. Intrinsic dimension estimation: advances and open problems. Inf Sci, 2016, 328: 26–41
40 Lindenbaum O, Yeredor A, Salhov M, et al. Multi-view diffusion maps. Inf Fusion, 2020, 55: 127–149
41 Granata D, Carnevale V. Accurate estimation of the intrinsic dimension using graph distances: unraveling the geometric complexity of datasets. Sci Rep, 2016, 6: 31377
42 Erba V, Gherardi M, Rotondo P. Intrinsic dimension estimation for locally undersampled data. Sci Rep, 2019, 9: 17133
43 Mo D Y, Huang S H. Fractal-based intrinsic dimension estimation and its application in dimensionality reduction. IEEE Trans Knowl Data Eng, 2012, 24: 59–71
44 Singer A, Erban R, Kevrekidis I G, et al. Detecting intrinsic slow variables in stochastic dynamical systems by anisotropic diffusion maps. Proc Natl Acad Sci USA USA, 2009, 106: 16090–16095
45 Cayton L. Algorithms for Manifold Learning. Technical Report, University of California, San Diego, 2005, 12: 1–17
46 Khanduri R, Rattan S S. Performance comparison analysis between IEEE 802. 11a/b/g/n standards. Int J Comput Appl Tech, 2013, 78: 13–20